United Nations S/2005/443

Security Council

Distr.: General
7 July 2005

Original: English

Letter dated 5 July 2005 from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

I write with reference to my letter of 3 May 2005 (S/2005/293). The Counter-Terrorism Committee has received the attached fourth report from Slovenia submitted pursuant to paragraph 6 of resolution 1373 (2001) (see annex). I would be grateful if you could arrange for the present letter and its annex to be circulated as a document of the Security Council.

(*Signed*) Ellen Margrethe **Løj**
Chairman
Security Council Committee established pursuant to
resolution 1373 (2001) concerning counter-terrorism

05-41734 (E) 040805

Annex

Letter dated 30 June 2005 from the Permanent Representative of Slovenia to the United Nations addressed to the Chairman of the Counter-Terrorism Committee

On the instructions of my Government and further to the letter dated 6 April 2005 from the Chairman, I have the honour to transmit the fourth report of the Republic of Slovenia on the implementation of counter-terrorism measures pursuant to Security Council resolution 1373 (2001) (see enclosure).

The Government of the Republic of Slovenia stands ready to provide any further information requested by the Counter-Terrorism Committee.

(*Signed*) Roman **Kirn**
Ambassador
Permanent Representative of the Republic of Slovenia
to the United Nations

Enclosure

The fourth report of the Republic of Slovenia on the implementation of counter-terrorism measures pursuant to Security Council resolution 1373 (2001)

I Implementation measures

Criminalisation of the financing of terrorism

1.1 The CTC welcomes the receipt of a progress report in relation to the amendment of the Penal Code, referred to on page 3 of the third report, that is intended to effectively implement subparagraph 1 (b) of the Resolution (as explained under question 1.2 of the CTC letter (S/AC.40/2002/MS/OC.224) dated 4 April 2003). If amendments were adopted, then please provide the CTC with copies thereof.

The Act Amending Criminal Code, which also includes a new criminal offence of terrorist financing, was adopted in April 2004 and published in the Uradni list Republike Slovenije (Official Gazette of the Republic of Slovenia), No. 40/04 of 20 April 2004.

The recently amended Criminal Code[1] is harmonised with the provisions of the International Convention for the Suppression of the Financing of Terrorism – hereinafter referred to as the "Convention")[2], which was ratified by the Republic of Slovenia in 2004.

The Act Amending the Criminal Code added Article 388a to the Criminal Code, which defines the criminal offence of financing terrorist activities. Paragraph 1 lists Articles of the Criminal Code defining criminal offences that are included in the criminal offence of financing terrorist activities. Other violent criminal offences are also added in compliance with the requirement of the Convention; these offences, however, must aim at destroying the constitutional order of the Republic of Slovenia, cause serious disruption to public life or the economy, cause death or serious physical injury to persons not actively involved in armed conflict, to intimidate people or force the state or an international organisation to act or fail to act.

Article 388a, paragraph 2 fulfils the requirement of the Convention to criminalise the collection of money for the purposes defined in paragraph 1 even if the money or property provided or collected was not used for the commission of such criminal offences.

Article 388a, paragraph 3 defines the aggravated form of the new criminal offence – the required condition is that it was committed within a criminal association.

In accordance with the systematics of the Criminal Code, paragraph 4 stipulates that such money and property must be seized.

Article 388a of the Criminal Code reads as follows:

"Financing of terrorist activities
Article 388a

(1) Whoever provides or collects money or property in order to partly or wholly finance commission of the criminal offences from Articles 144, 330, 331, 352, 353, 354, 355, 360, 388, 389 or 390 of this Code, or any other violent act whose objective is to destroy the constitutional order of the Republic of Slovenia, cause serious disruption to public life or the

[1] Ur. l. RS, No. 95/04 – officially consolidated text 1

[2] Act Ratifying the International Convention on the Suppression of the Financing of Terrorism, Ur. l. RS – MP, No. 21/04

economy, cause death or serious physical injury to persons not actively involved in armed conflict, to intimidate people or force the state or an international organisation to carry out an act or not to carry out an act shall be given a prison sentence of between one and ten years.

(2) Whoever commits an offence from the preceding paragraph shall be subject to the same penalty even if the money or property provided or collected was not used for commission of criminal offences specified in the preceding paragraph.

(3) If an offence from the preceding paragraphs was committed within a criminal association, the perpetrator shall be given a prison sentence of at least three years.

(4) Money and property from the preceding paragraphs shall be confiscated."

1.2 ***The CTC would also welcome receiving a progress report and an outline of the measures introduced to implement effectively subparagraph 1(c) of the Resolution that were noted at page 4 of the third report.***

The Republic of Slovenia has comprehensively regulated the domain of international sanctions by the Restrictive Measures Act (Ur. l. RS, No. 35/01) and the Act Amending the Restrictive Measures Act (Ur. l. RS, No. 59/02). The Act authorises the Government of the Republic of Slovenia to adopt decrees transposing international sanctions into Slovenian national legislation. On 23 January 2003, the Government of the Republic of Slovenia set up an Interdepartmental Working Group for the Implementation of Restrictive Measures and for the Monitoring of Activities relating to the Fight against Terrorism.

On the basis of the Restrictive Measures Act, the Government of the Republic of Slovenia has adopted:

- Decree on Measures Directed against Iraq,
- Decree on Measures Directed against UNITA,
- Decree on Measures against the Taliban (Afghanistan),
- Decree on Measures against the Federal Republic of Yugoslavia,
- Decree on the Expiration of the Decree on Measures Directed against UNITA (Angola),
- Decree Amending the Decree on Measures Directed against Iraq,
- Decree on Measures Directed against Sierra Leone,
- Decree on Measures Directed against Eritrea and Ethiopia,
- Decree on Measures Directed against Rwanda,
- Decree on Measures Directed against Liberia,
- Decree on Measures Directed against Somalia,
- Decree Amending the Decree on Measures Directed against the Taliban (Afghanistan).

The following draft decrees were submitted for consideration to the Government of the Republic of Slovenia in 2005 (situation as at 20 May 2005):

- Draft decree on the expiration of the Decree Directed against the Taliban,
- Draft decree concerning specific restrictive measures directed against certain persons and entities with a view to combating terrorism,
- Draft decree imposing certain specific restrictive measures directed against Usama bin Laden, the Al Kaida network and the Taliban and certain persons, groups, companies and entities associated with them,
- Draft decree on restrictive measures against Myanmar (Burma),
- Draft decree on restrictive measures against Zimbabwe,
- Draft decree on restrictive measures against Libia,
- Draft decree on restrictive measures against the Democratic Republic of Congo.

1.3 ***The CTC notes that according to Slovenia's response in relation to the questions of the regulation of alternative money transfers, and that these agencies do not exist in Slovenia (page 4 of the third report). In this regard, the CTC would appreciate receiving a further explanation as to how Slovenia identifies and ensures that alternative financial remittance systems are not taking place in Slovenia, at least, illegally. In case illegal alternative financial remittance operations have been identified by Slovenia, then please explain to the CTC what remedies and measures have been adopted to ensure that these illegal alternative financial remittance systems cease to operate.***

In Slovenia, money transfers may only be effected through banks and the Western Union international payment system, which is offered as a service by two banks and is effected only in branches of these two banks. The supervision over the operations of banks and other financial institutions is carried out by the Bank of Slovenia. To date, none of the Slovenian supervisory bodies or law enforcement authorities has detected an alternative financial remittance system, nor have these bodies received any information from abroad of the existence of such a system.

1.4 ***The CTC would welcome receiving a progress report on Slovenia becoming a party to the International Convention for the Suppression of the Financing of Terrorism.***

The Slovenian National Assembly ratified the Convention on 15 July 2004. The Republic of Slovenia deposited the instrument of ratification on 23 September 2004, the Convention entered into force in respect of Slovenia on 23 October 2004 (depositary's notification (references: C.N.979.2004, TREATIES-35 of 23 September 2004)).

Effectiveness in the protection of the financial system

1.5 ***The CTC would welcome receiving an outline of the changes and amendments to the Law on Criminal Proceedings, that pertain to the collection of confidential information from banks, saving banks and other institutions involved in financial transactions in cases related to the acquisition of information on international terrorism and its funding, as referred to in Slovenia's annex on "Information Exchange on the Code of Conduct on Political-Military Security Aspects".***

The request for explanation under the mentioned item refers to amendments to the Criminal Procedure Act [3]in the part referring to the acquisition of confidential information from financial organisations regarding the preliminary and criminal proceedings. The request also refers to the forwarding of the text of the relevant article of the Criminal Procedure Act.

In the Act on Amendments and Additions to the Criminal Procedure Act[4] from 2003, Article 156 was amended that stipulates the procedure for the acquisition of confidential information and documentation on financial transactions and other deals by the suspect or the defendant and also other persons, who may reasonably be presumed to have been implicated in the financial transactions or deals of the suspect or the defendant ("Production Order"). The investigating judge may, upon a properly reasoned proposal of the state prosecutor, order a bank, savings bank or savings-credit service to disclose to him such information. Article 156, paragraph 1 of the Criminal Procedure Act, stipulates among other conditions for interference with bank secrecy that the data required might represent evidence in criminal proceedings or are necessary for the seizure of objects or the securing of a request for the seizure of property benefits or the seizure of property whose value is equivalent to the value of property benefits.

[3] Ur. l. RS, No. 96/04 – officially consolidated text 2
[4] Ur. l. RS, No. 56/03.

Article 156, paragraphs 3 and 4 of the Act provides for the monitoring of suspect's transactions through his accounts with a financial organisation ("Monitoring Order"). For such an order, the same requirements must be met as for the order under paragraph 1, and refers to the current disclosure of information regarding transactions and deals (In the order, the investigating judge must set the time period within which the financial organisation must provide him with the data), which the suspect and other persons are carrying out or intend to carry out at financial organisations and who may reasonably be presumed to have been implicated in the transactions of the suspect or the defendant. The measure referred to may be applied for three months at most, but the term may, for weighty reasons, be extended to six months at most.

In compliance with Article 156, paragraph 5 the financial organisation may not disclose to its client or a third person that it has sent the data and documentation to the investigating judge.

The above Article 156 of the Criminal Procedure Act reads as follows:

"156. Article

(1) The investigating judge may upon a properly reasoned proposal of the public prosecutor order a bank, savings bank or savings-credit service to disclose to him information and send documentation on the deposits, statement of account and account transactions or other transactions by the suspect, the defendant and other persons who may reasonably be presumed to have been implicated in the financial transactions or deals of the suspect or the defendant, if such data might represent evidence in criminal proceedings or are necessary for the seizure of objects or the securing of a request for the seizure of property benefits or the seizure of property whose value is equivalent to the value of property benefits.

(2) The bank, savings bank or savings-credit service shall immediately send to the investigating judge the data and documentation referred to in the preceding paragraph.

(3) Subject to conditions from the first paragraph of this Article, the investigating judge may upon a properly reasoned proposal by the state prosecutor order a bank, savings bank or savings-credit service to keep track of financial transactions of the suspect, the defendant and other persons reasonably presumed to have been implicated in financial transactions or deals of the suspect or the defendant, and to disclose to him the confidential information about the transactions or deals the aforesaid persons are carrying out or intend to carry out at these institutions or services. In the order, the investigating judge shall set the time period within which the bank, savings bank or savings-credit service shall provide him with the data.

(4) The measure referred to in the preceding paragraph may be applied for three months at most, but the term may for weighty reasons, upon motion of the state prosecutor, be extended to six months at most.

(5) The bank, savings bank or savings-credit service may not disclose to their clients or third persons that they have sent, or will send, the data and documentation to the investigating judge."

1.6 ***Effective implementation of subparagraph 1 (a) of the Resolution requires States to have in place effective executive machinery for preventing and suppressing the financing of terrorist acts. In this context the CTC would like to know whether Slovenia provides its administrative, investigative, prosecutorial and judicial authorities with specific training aimed at enforcing its law in relation to:***

- ***typologies and trends aimed at countering terrorist financing methods and***

techniques;

- *techniques for tracing property, which represent the proceeds of crime or which are of legal origin but are to be used to finance terrorism, with a view to ensuring that such property is frozen, seized or confiscated?*

Please outline any relevant programs and/or courses. What mechanisms/programs has Slovenia put in place to train various financial sectors in the detection of unusual and suspicious financial transactions related to terrorist activities and in the prevention of the movement of illicit money?

Due to the absence of suitable practices in Slovenia, Slovenia's police in most cases apply foreign practices or good practices formulated abroad. On the basis of Slovenia's own practices and experience, which characterise its territory both at the national level and at the level of regional cooperation, specific guidelines were drawn up for:

- the area of terrorist financing, which covers its typologies and trends. They also include visibility elements and indicators, sources of financing and the methods of transfer of means. The key part of the guidelines is the preventive approach, which aims to detect the preparations on time, thus preventing the consequences and ensuring that the means are seized before they are channelled or transferred to another country;

- techniques for tracing property and seizure or confiscation of means originating from criminal offences as well as of means which are of legal origin but might be used for the preparation or implementation of terrorist activities regardless of the fact whether they have been generated from legal or illegal sources. An aide-memoire has been drafted, which covers the purpose of measures, the methods and sources for acquiring data, the methods and techniques for establishing unlawfulness, the methods for establishing the value of unlawful property benefits, the procedures of temporary securing of a request for the seizure of property benefits etc. Within regular annual training, particularly in the field of suppressing economic crime, additional training is planned in this field, which covers money laundering techniques or the use of some money laundering techniques for the purposes of financing terrorism or the transfer of means.

In the Republic of Slovenia, the education of judges, with the financial support by the justice education centre, is provided in terms of both organisation and implementation by the Supreme Court of the Republic of Slovenia; some courses are also organised annually by the Association of Judges and by higher courts. The education programme is formulated by the programme council of the justice education centre.

The courses have been organised for the eighth year in a row within the schools for judges, which are held for three consecutive days, several times a year. Each school is attended on average by 150 participants and the schools focus on different topics and issues in a certain area of law. The selected topics are particularly connected with resolving specific issues that occurred in practice and require in-depth expert examination, and also areas covered by the Act on Amendments and Additions to the Criminal Procedure Act and the Criminal Code.

Courses for state prosecutors are carried out within the schools for public prosecutors; they have the same content and are adapted to the powers and functioning of state prosecutors. Courses or consultations of state prosecutors relating to the above areas are also held in cooperation between the Supreme State Prosecutor's Office of the Republic of Slovenia and the Ministry of the Interior - General Police Directorate and the Office for Money Laundering Prevention.

At present, the Office of the Republic of Slovenia for Money Laundering Prevention has no legal competence in the field of detecting terrorist financing; it is only authorised for the

prevention, analysis and disclosure of suspicious transactions activity in connection with the criminal offence of money laundering. Certain powers relating to terrorist financing may be used by the Office only in case where grounds have been established for the suspicion of the criminal offence of money laundering, if this originates from a prior criminal offence of terrorist financing. In addition, the Office may, on the basis of Article 22, paragraph 3 of the Prevention of Money Laundering Act, when it begins collecting information regarding the suspected money laundering and it establishes, when analysing the data, information and documentation, that there are reasons to suspect, in connection with a transaction or a certain person, that the following serious criminal offences including terrorist financing or terrorism-related other criminal offences have been committed, forward written notification of its findings to the competent authorities (police, state prosecutor's office, Slovene Intelligence and Security Agency and some other state bodies).

The Office for Money Laundering Prevention will be given new powers in this area only after the act amending the Prevention of Money Laundering Act has been adopted. The Office and the Ministry of Finance will begin amending the Act immediately after the Third Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing has been adopted. The amendments to the Money Laundering Prevention Act, which will be adopted presumably by May 2006 at the latest, will stipulate that all reporting agents under the Act shall notify the Office of suspicious transactions in the field of terrorist financing. Thus, the Office would become a central point for receiving information on suspicious transactions relating to terrorist financing and for international cooperation in this field.

Despite the fact that the Office is not yet exercising the powers it is to acquire only after the Money Laundering Prevention Act has been amended, it is has the required expertise in this field, as several Office employees in the last four years participated in a number of seminars and other forms of education, which were held in Slovenia and abroad under the auspices of international organisations in the field of prevention and detection of terrorist financing. With regard to these issues, two Office representatives also hold lectures and formulate assessments for the Council of Europe (within the MONEYVAL Committee of Experts) in assessing the measures in the field of money laundering and terrorist financing in other countries.

In October 2004, Slovenia hosted a two-day international seminar on the prevention and detection of money laundering and terrorist financing. The seminar was organised by the Council of Europe, Office for Money Laundering Prevention and the Regional Institute - Centre of Excellence in Finance of the Ministry of Finance in cooperation with the Bank of Slovenia and the Securities Market Agency of the Republic of Slovenia. The seminar was attended by more than 60 representatives of money laundering prevention agencies, supervisory bodies and the police, central banks and bank associations from 12 countries. The seminar focused on the tasks of government offices and supervisory bodies in the field of banking and securities market in the prevention and detection of money laundering and terrorist financing. Two representatives of the Slovenian Office participated as lecturers.

In June 2002, the General Police Directorate organised a seminar in Ljubljana on financial investigations for criminal police staff members, which was also attended by representatives of the Office for Money Laundering Prevention.

1.7 ***Regarding the suppression of the financing of terrorism, as required by subparagraph 1 (a) of the Resolution, the CTC would appreciate learning whether the Office for Money Laundering Prevention, referred to at page 8 of the third report, has sufficient resources (human, financial, technical) to enable it to carry out its mandate. Please provide appropriate data in support of your response.***

The Office for Money Laundering Prevention employs 17 persons, six of which work in the area of suspicious transactions and analytics, three in the field of prevention, two in the field of information technology, one in the field of international cooperation, three in the Office management and two in the secretariat.

There is no special organisation unit or post specialised only in detecting criminal offences of terrorist financing. Nevertheless, the Office has all required resources (human, financial, technical) and expertise in this field to enable it to carry out its mandate, although the team will have to be enhanced with at least two new members in the following two years owing to the increased amount of work.

1.8 ***In relation to the Money Laundering Act of 25 October 2001 and the Office for Money Laundering Prevention, would Slovenia please provide the CTC with the number of suspicious transaction reports (STRs) received by the Office from the following institutions which are covered by the above Money Laundering Act, as indicated at page 4 of the first report:***

- ***Financial institutions;***
- ***Notaries;***
- ***Accountants;***
- ***Auditors; and***
- ***Tax consultants.***

Please indicate the number of STRs analysed and disseminated, as well as the number of STRs that have led to investigations, prosecutions or convictions.

The number of suspicious transactions reports (STRs) or processed cases

The Office for Money Laundering Prevention may start processing a case only if grounds exist for suspicion that money laundering in connection with a transaction or a person has been committed (also if grounds exist for suspicion of money laundering regarding money originating from the criminal offence of financing terrorist activities), and under the following conditions:

- if under Article 20 of the Prevention of Money Laundering Act, the Office receives a substantiated initiative in writing from the following state bodies (courts, State Prosecutor's Office, police, Slovene Intelligence and Security Agency, Bank of Slovenia, Securities Market Agency, Insurance Supervision Agency, or inspectorate bodies of the Ministry of Finance) provided that grounds exist for suspicion of money laundering in connection with a transaction or a person,
- if it is notified of suspicious (cash or non-cash) transactions regardless of the amount and of cash or several connected cash transactions exceeding SIT 5,000,000.00 by financial and other organisations - reporting agents under Article 10 of the Prevention of Money Laundering Act,
- if it is notified under Article 28 of the Prevention of Money Laundering Act of suspicious transactions by a lawyer, law firm, notary, an audit company, an independent auditor or legal or natural person performing accountancy services or tax advisory services,
- on the basis of a request by foreign agencies (FIU - Financial Intelligence Units), other competent foreign authorities and international organisations,
- on the basis of information on cash or securities transfer to the bearer, forwarded to the Office by the Customs Administration of the Republic of Slovenia,
- on the basis of other information collected by the Office on the basis of the provisions of the Prevention of Money Laundering Act.

The number of processed cases by reporting agents in the period 2000-2004 is given in the table below:

REPORTING AGENTS	2000	2001	2002	2003	2004
1. Organisations under Article 2 of the Prevention of Money Laundering Act-1	65	48	47	41	84
	68.4 %	59.2 %	51.1 %	51.9%	74.3%
Banks	55	41	41	37	74
Savings banks				2	2
Agency for Payment Transactions	2	2			
Exchange offices	3		1		
Post of Slovenia		3	1		
Ljubljana Stock Exchange	4	2			
Stock broking firms			2	2	3
Management companies			1		1
Leasing organisations			1		
Real estate organisations	1				
Gaming house					3
Tourist agency					1
2. Reporting agents under Article 28 of the Prevention of Money Laundering Act-1			2	5	1
			2.2 %	6.3%	0.9%
Auditors			1	2	
Accounting agencies			1	2	
Notaries				1	1
3. INITIATIVES OF STATE BODIES UNDER ARTICLE 20 OF THE PREVENTION OF MONEY LAUNDERING ACT-1	17	16	26	21	18
	17.9 %	19.8 %	28.3 %	26.6%	16.0%
Ministry of the Interior, Criminal Police Directorate	14	13	14	18	5
State Prosecutor's Office	1		2		1
Court					1
Ministry of Finance - Tax Administration of the Republic of Slovenia	2	1	6		1
Ministry of Finance - Customs Administration of the Republic of Slovenia				1	1
Ministry of Finance - Foreign Exchange Inspectorate of the Republic of Slovenia		2	2		1
Bank of Slovenia				1	5
Slovene Intelligence and Security Agency (SOVA)			2	1	1
Securities Market Agency					2
4. SET ASIDE BY THE OFFICE OUT OF CASH ABOVE SIT 5,000,000.00	2	2	4	2	1
	2.1 %	2.5 %	4.3 %	2.6%	0.9%
5. AGENCIES OF OTHER COUNTRIES AND INTERNATIONAL ORGANISATIONS	11	15	13	10	9

	11.5 %	18.5 %	14.1 %	12.6%	7.9%
TOTAL:	95	81	92	79	113

In 2001, the Office joined, within its competences, international and domestic activities in the field of combating terrorism, particularly in the part referring to the prevention and detection of terrorist financing. These activities continued also in 2002, 2003 and 2004. In terms of content, the activities were also aimed at cross checking certain persons on the lists of the UN Security Council and the EU, or persons, who were reported to the Office by foreign agencies as persons connected with terrorism. Thus, in the period 2001-2004, the total of 7,649 different legal or natural persons were cross checked in the records of the Office, who were suspected of being connected with terrorism. It was established that none of the persons that were checked had carried out or been connected with financial transactions in the Republic of Slovenia.

The number of cases analysed and the number of cases forwarded to the competent authorities

During the 1995-2004 period, the Office analysed and concluded 655 cases out of 765 cases received. As regards concluded cases, the Office submitted the 127 cases in which additional collecting and analysing the data showed that there were certain grounds for suspicion of committing the criminal offence of money laundering, and the relevant documentation on the basis of Article 22 of the Prevention of Money Laundering Act, for further consideration to the Criminal Police Directorate of the Ministry of the Interior, in certain cases also to the competent State Prosecutor's Office. The Act Amending the Prevention of Money Laundering Act (Ur. l. RS, No. 59/02) of 25 October 2001 enabled the Office to notify the competent state bodies not only of suspected money laundering but also of suspected other criminal offences. Since then, in addition to notifications of suspicious transactions, 59 notices of written information on the grounds of alleged other criminal offences have been submitted to the competent authorities. When there are grounds of alleged other more serious criminal offences including terrorist financing or other criminal offences connected with terrorism, the Office may, in respect of a transaction or a certain person, submit its findings in writing to the competent authorities (police, State Prosecutor's Office, Slovene Intelligence and Security Agency and other state bodies). So far, none of the information notices submitted related to criminal offences connected with terrorism. 469 cases, in which the initial suspicion of the criminal offence of money laundering or other criminal offences has not been confirmed, were filed by the Office as closed cases.

The number of cases in which criminal procedure was instituted

In the period from 1995 to 2004, the Office notified the Criminal Police Directorate of the Ministry of the Interior and/or the State Prosecutor's Office of suspicious transactions or circumstances in 127 cases. The data of the Criminal Police Directorate of the Ministry of the Interior show that the competent police directorates at that time filed a total of 47 criminal reports against 129 natural persons on the grounds of well-founded suspicion of having committed the criminal offence of money laundering under Article 252 of the Criminal Code. In the period from 1995 to 2004, 31 criminal reports (or 66%) out of 47 were based on the data received by the Office on suspicious transactions.

The data forwarded by the Police, state prosecutor's offices and courts show that proceedings regarding the 47 filed criminal reports were in the following phases as at 31 December 2004:

- 12 criminal reports (or 25.5% of all reports) were dismissed by the State Prosecutor's Office,
- the State Prosecutor's Office has not yet adopted a decision in respect of 2 criminal reports (or 4.2%),
- on the basis of 1 criminal report (or 2.1% of all reports) the State Prosecutor's Office filed a

request to initiate an investigation,

- on the basis of 10 criminal reports (or 21.2% of all reports), the examining judges initiated or concluded the investigation,
- on the basis of 7 criminal reports (or 14.9% of all reports) the State Prosecutor's Office filed indictments after the concluded investigation,
- on the basis of 3 criminal reports (or 6.4%), the prosecutors dropped the prosecution in two cases after the concluded investigation due to the lack of evidence, and in one case in the phase of investigation, as it was established that no criminal offence was committed,
- on the basis of 2 criminal reports (or 4.2% of all reports) the cases fell under the statute of limitations in the phase of indictment,
- on the basis of 3 criminal reports (or 6.4% of all reports) the courts pronounced final judgments of acquittal,
- on the basis of 3 criminal reports (or 6.4% of all reports) first-instance courts pronounced two judgements of conviction and one judgement of acquittal against three persons, As regards the judgement of acquittal, the State Prosecutor's Office filed an appeal, whereas the status of first-instance judgements of conviction is as follows: In one case, in which the first-instance judgement of conviction was set aside by the higher court, the defendant died and in 2004, the proceedings against him were therefore stopped. In the second case, in which the District Court pronounced the judgement of conviction at first instance, the judgement was reversed due to procedural defects by a decree of the higher court and returned to the District Court for reconsideration,
- on the basis of 4 criminal reports (or 8.5%), the courts, themselves or on proposal of the State Prosecutor's Office, proposed that criminal cases be assigned to another country, thus concluding the proceedings in Slovenia.

The proceedings have thus been concluded in 25 cases (criminal report dismissed in 12 cases, prosecution dropped in 3 cases, absolute limitation in 2 cases, final judgements of acquittal in 3 cases, proceedings stopped due to the death of the defendant 1 case and assignment of 4 cases to another country), 22 cases are still in different stages of proceedings.

Effectiveness of Counter-Terrorism Machinery

1.9 ***Effective implementation of legislation covering the various aspects of the Resolution requires States to have in place effective and coordinated executive machinery, as well as to create and utilize adequate domestic and international anti-terrorist strategies. In this regard, the CTC would appreciate knowing whether the Integrated Counter-Terrorism Strategy and/or the Plan of Detecting and Preventing Terrorist Activities in the territory of Slovenia deal with the following forms or aspects of counter terrorist activity:***

- ***Criminal investigation and prosecution;***
- ***Counter-terrorist intelligence (human and technical);***
- ***Special forces operations;***
- ***Physical protection of potential terrorist targets;***
- ***Strategic analysis and forecasting of emerging threats.***

To the extent possible, could Slovenia outline corresponding mechanisms, administrative procedures and best practices in this regard, which may not infringe upon any confidential information that may jeopardize the effectiveness of Slovenia's efforts to combat terrorism.

In the Republic of Slovenia, the field of anti-terrorism is covered by two intelligence and security agencies:

- Slovene Intelligence and Security Agency (SOVA),
- Intelligence and Security Service of the Ministry of Defence.

The Slovene Intelligence and Security Agency (SOVA) is a government agency directly responsible to the Prime Minister. In the field of anti-terrorism, it focuses particularly on collecting and analysing data and information on the preparations for and the commitment of terrorist and other violent acts by organisations and groups, which might be carried out in the territory of the Republic of Slovenia or by abusing its territory. Within its intelligence activity, the Agency also collects data by secret cooperation (Humint) and special forms of acquiring information (Sigint), e.g. following the international communications systems.

The Agency carries out its tasks in compliance with the Slovene Intelligence and Security Agency Act (Ur. l. RS, No. 20/04) and informs of its findings the Prime Minister and also the following persons, when matters fall under their competence:

- President of the Republic,
- President of the National Assembly,
- competent ministers, and
- other senior officials.

SOVA also forwards to the competent ministers and other officials the information of their field of work so that the competent authorities might propose or adopt certain measures. SOVA collects information and drafts analyses in their field of work for the requirements of the National Security Council.

If the Agency, in carrying out its duties set out in the Slovene Intelligence and Security Agency Act, establishes that grounds exist for suspicion that a certain person has committed or is preparing or organising a criminal offence (in this case a terrorist activity or providing logistic support for terrorist purposes) in respect of which prosecution is commenced ex officio, it is bound to notify the competent authorities, as it has no executive authority itself.

In its work, SOVA cooperates in this area with the Ministry of the Interior and the Police, the Ministry of Defence and if necessary, also with the competent State Prosecutor's Office or other competent institutions (e.g. the Office for Money Laundering Prevention).

In Compliance with the Act and according to the decision of its Director, the Agency cooperates or exchanges data with foreign intelligence and security agencies. The field of anti-terrorist fight is one of those in which the Agency established links and a range of bilateral relations with foreign agencies, with which it successfully exchanges data on the issues relating to terrorism, thus contributing to ensuring collective security.

Strategic analysis and forecasting of emerging threats

Most strategic analyses and assessments of threats to Slovenia associated with international terrorism are carried out by SOVA and, to a lesser extent, by the Ministry of the Interior/Police. As part of its activities, SOVA drafts assessments and analyses on the threat of Islamic terrorism in the region (Western Balkans), communicating information to the Prime Minister and relevant ministers and partner services.

The work of a special interdepartmental working group on combating transnational threats is of particular importance in this field, as it drafts regular and up-to-date assessments on threats to the state associated with international terrorism. It mostly focuses on Islamic extremism. The interdepartmental group includes the following institutions:

- SOVA (conducts and coordinates the group's work)
- Ministry of the Interior,
- Ministry of the Interior – Police,

- Ministry of Justice,
- Ministry of Foreign Affairs,
- Intelligence and Security Service of the Ministry of Defence,
- General Staff of the Slovenian Armed Forces,
- Ministry of Finance - Office of the Republic of Slovenia for Money Laundering Prevention,
- Ministry of Finance - Customs Administration of the Republic of Slovenia.

The Republic of Slovenia does not have an anti-terrorist strategy; it is currently being drawn up. However, individual departments take concerted action in combating international terrorism, *inter alia* through possibilities provided by a model and structure of operation of the National Security Council and particularly the interdepartmental working group on combating transnational threats.

For the scope it covers, the Police have a concept of work such as planned criminal intelligence activity, which includes a relevant response of analytics and thus enables the assessment of threats; a procedure that is coordinated and conducted by a relevant state prosecutor's office; and criminal investigation and law-enforcement.

The plan of activities includes the physical protection of potential terrorist targets. To this end, potential targets have been determined in cooperation with other departments according to the level of threats and the type of target (soft/hard), and an appropriate method of protection has been selected.

Since Slovenia has to date no experience with terrorist attacks, it would be difficult to identify cases of good practices. We endeavour to take advantage of practices of other countries, which are then adapted to the needs characterised by the fight against terrorism in Slovenia.

In specific cases, the manner of work has proven appropriate, particularly in the procedures of efficient border control and intense international cooperation.

The Slovenian police have drafted an action plan, including the methods to elaborate threat assessments, which depend on the area and danger of a particular phenomenon. The plan comprises all measures of internal organisational police units (Special Unit, Uniformed Police, Criminal Investigation Police, Operation and Communications Centres, Forensic Research Centre, and Security and Protection Bureau) considering the level of threats, which can be low, medium or high.

Tasks associated with the fight against terrorism are carried out within the basic tasks of the Slovenian Armed Forces, which include the following:

- implementing military defence of the Republic of Slovenia;
- protecting persons and facilities of particular importance for defence, and all military personnel, units and facilities that fall within the competence of the Slovenian Armed Forces;
- protection of the air space, and
- providing assistance to civil institutions in removing consequences of terrorist attacks.

The Act Amending the Defence Act (Ur. l. RS, No. 40/04) stipulates that important energy, transport, production, telecommunications and other similar facilities and headquarters of state authorities may be identified in the plans for the use of the army as being of significance for the state defence. Their protection, including the air space over these facilities, coast, and pertaining aquatorium in front of these facilities, is provided by the Slovenian Armed Forces in accordance with plans and preliminary approval of the Government.

The Slovenian Armed Forces may cooperate with the police in wider protection of the state border in the inner part of the state territory according to plans and after the approval of the Government.

The activities from the above provisions of the Defence Act mostly refer to the activities the Slovenian Armed Forces could carry out in the fight against terrorism.

At the strategic level, the post of the deputy chief of staff for the fight against terrorism is provided for in the General Staff of the Slovenian Armed Forces. His main responsibilities comprise coordination of all activities and the drafting of strategic guidelines for the fight against terrorism within the Slovenian Armed Forces.

The military police is responsible for military order and discipline, security of military traffic and certain tasks associated with prevention, investigation and detection of criminal offences in the army, protection of facilities and areas that are of special importance for defence. The military police can investigate criminal offences in the army for which the law prescribes a fine or prison sentence for no more than three years. The military police is also in charge of protecting military and civil persons discharging duties in the Slovenian Armed Forces and of special significance for defence; military delegations, commands and units, and protecting chief commander in case of a state of war or when he is in military commands, units or institutions or facilities and its surroundings that are of particular significance for defence.

The main tasks associated with the fight against terrorism in the Slovenian Armed Forces are carried out by staff intelligence security bodies and the battalion of the military police that also have appropriate legal basis in the Defence Act.

In cooperation with the Administration for Civil Protection and Disaster Relief of the Republic of Slovenia, the Slovenian Armed Forces are also used for eliminating consequences of a terrorist attack.

1.10 ***Effective implementation of subparagraph 2 (e) of the Resolution requires each Member State, inter alia, to have in place effective police, intelligence and/or other structures as well as adequate legal provisions to detect, monitor and apprehend those involved in terrorist activities and those supporting terrorist activities, with a view to ensuring that those persons are brought to justice. In this context. please indicate which special investigative techniques can be used in Slovenia in cases of terrorism (e.g. interception of communications; electronic surveillance; observation; undercover operations; controlled delivery; anonymous informants; cross-border pursuits, the electronic bugging of private or public premises etc.). Please explain the legal conditions that govern their use. Please specify whether they may only be applied to suspects and whether a court must first sanction their use. Please also specify the period of time for which they may be used. Could Slovenia also indicate whether the special investigative techniques can be used in cooperation with another State?***

Since Slovenia does not have special legislation for the field of terrorism, it applies mutatis mutandis the provisions of the Criminal Procedure Act, defining secret surveillance measures:

Secret surveillance (Article 149a of the Criminal Procedure Act)

(1) If there are reasonable grounds for suspecting that a certain person has committed, is committing, is preparing to commit or is organising the commission of any of the criminal offences specified in the fourth paragraph of this article and if it is reasonable to conclude that police officers would be unable to uncover, prevent or prove this offence using other measures, or if these other measures would give rise to disproportionate difficulties, secret surveillance of this person may be ordered.

(2) Secret surveillance may also exceptionally be ordered against a person who is not a suspect if it is reasonable to conclude that surveillance of this person will lead to the identification of a suspect from the preceding paragraph whose personal data is unknown, to the residence or whereabouts of a suspect from the preceding paragraph, or to the residence or whereabouts of a person who was ordered into custody, ordered to undergo house arrest or had an arrest warrant or an order to appear issued against him but who escaped or is in hiding and police officers are unable to obtain this information by other measures, or if these other measures would give rise to disproportionate difficulties.

(3) Secret surveillance shall be carried out as continual or repeat sessions of surveillance or pursuit using technical devices for establishing position or movement and technical devices for transmitting and recording sound, photography and video recording, and shall focus on monitoring the position, movement and activities of a person from the preceding paragraphs. Secret surveillance may be carried out in public and publicly accessible open and closed premises, as well as places and premises that are visible from publicly accessible places or premises. Under conditions from this article, secret surveillance may also be carried out in private premises if the owner of these premises so allows.

(4) The criminal offences for which secret surveillance may be ordered are as follows:

1) criminal offences for which the law prescribes a prison sentence of five or more years;
2) criminal offences from point 2 of the second paragraph of Article 150 of this Act and the criminal offences of false imprisonment (Article 143 of the Penal Code), threatening the safety of another person (Article 145), fraud (Article 217), concealment (Article 221), disclosure of and unauthorised access to trade secrets (Article 241), abuse of inside information (Article 243), fabrication and use of counterfeit stamps of value or securities (Article 250), forgery (Article 256), special cases of forgery (Article 257), abuse of office or official rights (Article 261), disclosure of an official secret (Article 266), being an accessory after the fact (Article 287), endangering the public (Article 317), pollution and destruction of the environment (Article 333), bringing of hazardous substances into the country (Article 335), pollution of drinking water (Article 337), and tainting of foodstuffs or fodder (Article 338).

(5) Secret surveillance shall be permitted by the state prosecutor on the basis of a written order and at the written request of the police, except in cases from the sixth paragraph of this article, when an order must be obtained from the investigating judge.

(6) Secret surveillance shall be ordered in writing by the investigating judge, at the written request of the state prosecutor, in the following cases:

1) if he envisages the use of technical devices for the transmission and recording of sound in the application of the measure, where this measure may be ordered only for criminal offences from the second paragraph of Article 150 of this Act;
2) if application of the measure requires the installation of technical devices in a vehicle or in other protected or closed premises or objects in order to establish the position and movements of a suspect;
3) for application of a measure in private premises, if the owner of these premises so allows;
4) for the application of a measure against a person who is not a suspect (second paragraph of this article).

(7) Requests and orders shall be constituent parts of criminal case records and must contain:

1) information that allows the person against whom the measure is being requested or ordered to be identified accurately;
2) reasonable grounds or the adducement of reasonable grounds for suspicion;

3) in the case from the second paragraph of this article, information that allows a suspect from the first paragraph of this article to be identified accurately, and the establishment of probability that application of the measure will lead to the identification of the suspect, his whereabouts or his place of residence;
4) the written consent of the owner of the private premises in which the measure will be applied;
5) the method of application, the scope and the duration of the measure, and other important circumstances that dictate use of the measure;
6) the grounds for or establishment of need to use the measure in question as opposed to another method of gathering information.

(8) In exceptional cases, if written orders cannot be obtained in time and if a delay would present a risk, the state prosecutor may, in the case from the fifth paragraph of this article and at the verbal request of the police, allow the measure to commence on the basis of a verbal order; in the case from the sixth paragraph of this article, the investigating judge may, at the verbal request of the state prosecutor, allow the measure to commence on the basis of a verbal order. The body that issued the verbal order shall make an official note of the verbal request. A written order, which must contain the reason why the measure has been commenced before time, must be issued within 12 hours of the issuing of the verbal order at the latest. Reasonable grounds must exist for application of the measure before time; if this is not the case, the court shall always act in accordance with the fourth paragraph of Article 154 of this Act regardless of whether the use of measures is otherwise justified.

(9) If a person against whom a measure is being applied comes into contact with an unidentified person in relation to whom there are reasonable grounds for suspecting that he is involved in criminal activity connected with the criminal offences for which the measure is being applied, the police may also place this person under secret surveillance without the need to obtain the order from the fifth or sixth paragraphs of this article if this is urgently required in order to establish the identity of this person or obtain other information important for criminal proceedings. The police must obtain prior verbal permission from the state prosecutor for such surveillance, unless it is impossible to obtain permission on time and any delay would present a risk. In this case the police shall, as soon as possible and within six hours of commencement of application of the measure at the latest, inform the state prosecutor, who may prohibit further application of the measure if he believes that there are no reasonable grounds for it. This measure may last for a maximum of 12 hours from contact with the person against whom the measure is being applied. When applying the measure from this paragraph, the police may not use technical equipment and devices from points 1 and 2 of the sixth paragraph of this article, nor may they apply the measure in private premises. The police shall make an official note immediately after the cessation of such surveillance and send it without delay to the state prosecutor that granted the permission from this paragraph and to the body that issued the original secret surveillance order. The official note shall become part of the criminal case records.

(10) Application of a measure may last a maximum of two months; if due cause is adduced, it may be extended every two months by means of a written order. The measure may last a total of:

1) six months in the case from the sixth paragraph of this article;
2) 24 months in cases from the fifth paragraph of this article if they relate to criminal offences from the fourth paragraph of this article, and 36 months if they relate to criminal offences from the second paragraph of Article 151 of this Act.

(11) The police shall cease to apply the measure as soon as the reasons for which the measure was ordered are no longer in place. The police shall notify the body that ordered the measure of the cessation without delay and in writing. The police shall send the body that ordered the

measure a monthly report on the progress of the measure and the information obtained. The body that ordered the measure may, at any time and on the basis of this report or *ex officio*, order in writing that application of the measure be halted if it assesses that the reasons for the measure are no longer in place or if the measure is being applied in contravention of its order.

(12) If a measure is applied against the same person for more than six months, the panel (sixth paragraph of Article 25) shall review the legality of and grounds for application of the measure upon the first extension over six months and every further six months thereafter. The body that issued the extension order shall send the panel all the relevant material; the panel shall decide within three days. If the panel assesses that there are no grounds for application of the measure or that all the legal conditions have not been fulfilled, it shall issue a decision ordering that the measure come to an end. There shall be no appeal against this decision.

(13) The police must carry out secret surveillance in a way that encroaches on the rights of persons that are not suspects to the smallest possible extent.

Identification of users of means of electronic communication (Article 149b of the Criminal Procedure Act)

(1) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the state prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish him with information on the participants in and the circumstances and facts of electronic communications, such as: number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.

(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an adducement of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.

(3) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may demand that the operator of the electronic communications network furnish it with this information, at its written request and even without the consent of the individual to whom the information refers.

(4) The operator of electronic communications networks may not disclose to its clients or a third party the fact that it has given certain information to an investigating judge (first paragraph of this article) or the police (preceding paragraph), or that it intends to do so.

Monitoring of electronic communications (Article 150 of the Criminal Procedure Act)

(1) If there are well-founded grounds for suspecting that a particular person has committed, is committing or is preparing or organising the committing of any of the criminal offences listed in the second paragraph of this article, and if there exists a well-founded suspicion that such

person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not permit the gathering of data or that the gathering of data could endanger the lives or health of people, the following may be ordered against such person:

1) the monitoring of electronic communications using bugging and recording devices and the control and protection of evidence on all forms of communication transmitted over the electronic communications network;
2) control of letters and other parcels;
3) control of the computer systems of banks or other legal entities which perform financial or other commercial activities;
4) bugging and recording of conversations with the permission of at least one person participating in the conversation;

(2) The criminal offences in connection with which the measures from the previous paragraph may be ordered are:

1) criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international law for which the law prescribes a prison sentence of five or more years;
2) the criminal offence of kidnapping under Article 144, the showing, possession, manufacture and distribution of pornographic material under Article 187, illegal production of and trade in drugs under Article 196, enabling the taking of drugs under Article 197, blackmail under Article 218, abuse of inside information under Article 243, unauthorised acceptance of gifts under Article 247, unauthorised giving of gifts under Article 248, money laundering under Article 252, smuggling under Article 255, accepting of a bribe under Article 267, giving of a bribe under Article 268, acceptance of gifts to secure unlawful intervention under article 269, giving of gifts to secure unlawful intervention under Article 269a, criminal association under Article 297, unauthorised production of and trade in arms or explosives under Article 310, and causing danger with nuclear substances under the third paragraph of Article 319 of the Penal Code of the Republic of Slovenia;
3) other criminal offences for which the law prescribes a prison sentence of eight or more years.

Bugging and surveillance in other person's home or in other areas (Article 151 of the Criminal Procedure Act)

(1) If there exist well-founded reasons to suspect that a particular person has committed, is committing, or is preparing or organising the committing of any of the criminal offences listed in the second paragraph of this article, wherein it is possible to reasonably conclude that it will be possible in a precisely defined place to obtain evidence which more lenient measures, including the measures from Articles 149a, 149b and 150 of this Act, would not be able to obtain or the gathering of which could endanger the lives of people, exceptionally bugging and surveillance in another person's home or in other areas with the use of technical means for documentation and where necessary secret entrance into the aforementioned home or area may be ordered against such a person.

(2) Measures from the previous paragraph may be ordered in connection with all criminal offences from the first point of the second paragraph of the previous article, criminal offences from the second point of the same paragraph, except for the criminal offence of kidnapping under Article 144, enabling the taking of drugs under Article 197, blackmail under Article 218, money laundering under the first, second, third and fifth paragraphs of Article 252 and smuggling under Article 255 of the Penal Code of the Republic of Slovenia, and in connection with other criminal offences from the third point of the same paragraph for which the law

prescribes a prison sentence of eight or more years only if there exists a real danger to the lives of people.

Undercover operations (Article 155a of the Criminal Procedure Act)

(1) If there are reasonable grounds for suspecting that a certain person has committed any of the criminal offences from the fourth paragraph of Article 149a of this Act, or if it is reasonable to conclude that a certain person is involved in a criminal activity connected with the criminal offences from the fourth paragraph of Article 149a of this Act and that other measures will not yield evidence or will give rise to disproportionate difficulties, undercover operations may be used against this person.

(2) Undercover operations shall be carried out by undercover operatives and involve the continual gathering of information or repeat sessions of information gathering on a person and his criminal activities. Undercover operations shall be carried out by one or more undercover operatives under the direction and supervision of the police, using false information about an operative, false information in databases and false documents in order to prevent the information gathering process or the status of the operative from being disclosed. An undercover operative may be a police officer, a police employee of a foreign country or exceptionally, if undercover operations cannot be carried out in any other way, by another person. An undercover operative may, under conditions from this article, participate in legal transaction using false documents; when information is being gathered under the conditions from this article, technical devices for transmitting and recording sound, photography and video recording may also be used.

(3) An undercover operation measure shall be permitted by the state prosecutor on the basis of a written order and at the written request of the police, except in cases from the fourth paragraph of this article, where the order must be issued by the investigating judge. The order may also encompass permission to manufacture, obtain and use false information and documents.

(4) An undercover operation measure where the undercover police employee will use technical devices for transmitting and recording sound, photography and video recording may only be ordered in connection with criminal offences from the second paragraph of Article 150 of this Act. The measure shall be ordered by the investigating judge in writing, at the written request of the state prosecutor.

(5) Requests and orders shall be constituent parts of criminal case records and must contain:

1) information that allows the person against whom the measure is being requested or ordered to be identified accurately;
2) reasonable grounds or the adducement of reasonable grounds for suspicion;
3) the method of application, the scope and the duration of the measure, and other important circumstances that dictate use of the measure;
4) the type, purpose and scope of use of false information and documents;
5) if the undercover operative will take part in legal transactions, the permitted scope of this participation;
6) if the undercover operative is not a police officer or police employee from another country but another person, the adducement of reasonable grounds for deploying this person;
7) in the case from the preceding paragraph, determination of the type and method of use of technical devices for transmitting and recording sound, photography and video recording;
8) the grounds for or establishment of need to use the measure in question as opposed to another method of gathering information.

(6) Application of the measure may last a maximum of two months. If due cause is adduced, it may be extended every two months by means of a written order, but to a maximum of 24 months. In the case of the use of a measure for criminal offences from the second paragraph of Article 151 of this Act, the maximum duration shall be 36 months.

(7) The provisions of the eleventh and twelfth paragraphs of Article 149a of this Act shall be applied *mutatis mutandis* to the cessation of application of undercover operations, the compilation of monthly reports by the police and the review of extension by the panel (sixth paragraph of Article 25).

(8) Measures from this article must be carried out in a way that encroaches on the rights of persons that are not suspects to the smallest possible extent.

(9) When carrying out a measure, an undercover police officer may not encourage criminal activity. The provisions of the third and fourth paragraphs of Article 155 of this Act shall be applied *mutatis mutandis* to encouraging criminal activity.

SOVA also collects information through covert cooperation and special forms of information collection, whereby the director of the agency determines, with the approval of the Government, the conditions and methods of information collection through covert cooperation, as well as procedures and measures for the protection of sources.

Under the conditions stipulated by the Act, the agency may use the following special forms of information collection in order to discharge its functions:

- monitoring of international communications systems,
- covert purchase of documents and objects,
- covert observation and surveillance in open and public places applying technical means for documenting,
- interception of letters and other means of communication, and the interception of telecommunications.

Monitoring of international communications systems, covert observation and surveillance in open and public places, applying technical means for documenting, and covert purchase of documents and objects are authorised by the director of SOVA.

At the request of the director of SOVA, the interception of letters and other means of communication, and the interception of telecommunications are authorised by a written order issued by the president of the district court with jurisdiction in the area where SOVA's headquarters are based. The application of this special form of information collection may not exceed three months. If reasonable grounds exist, its application may be extended in one month increments, but not to exceed six months in total.

The data collected through special forms cannot be used as evidence in court. In accordance with Article 8 of the Act, if the Agency establishes that grounds exist for suspicion that a certain person has committed or is committing a criminal offence, or is preparing or organising a criminal offence subject to prosecution *ex officio*, it is bound to notify the Director General of the Police and the competent state prosecutor thereof.

The SOVA Act contains no reservation regarding cooperation with another country in the field of special forms of information collection. Each implementation of these forms of information collection has to be approved in accordance with the SOVA Act. In exchanging information, the Personal Data Protection Act has to be considered (Ur. l. RS, No. 86/2004).

1.11 With a view to bringing terrorists and their supporters to justice, please indicate whether Slovenia has taken any measures to protect vulnerable targets in terrorist cases, (for example, victims, witnesses or other persons assisting the court, judges and prosecutors). Please describe the legal and administrative provisions that Slovenia has put in place to ensure this protection.

The protection of the above persons is partially regulated by the Criminal Procedure Act; its article 240a determines the procedure to provide anonymity concerning the hearing before the investigating judge and at the main hearing; its article 141a provides legal basis for the drafting and enforcement of the law regulating the protection of witnesses and persons regretting their acts in the police procedure, during and after criminal proceedings, based on the comprehensive programmes of witness protection.

Article 141a of the Criminal Procedure Act determines that the condition to acquire protection within the protection programme is met when there are grounds for believing that lives of a witness or person regretting his/her act (person who cooperate with law enforcement of judicial authorities; so called repentant or pentiti) and their immediate family are in danger as a consequence of their testimony. Amendments to the Criminal Procedure Act, drafted by the Ministry of Justice, will replace "grounds for believing that lives ... are endangered" with "serious danger for life and body", which will extend the possibilities of providing protection within comprehensive protection programmes. This article also determines that measures within the protection programme are provided at the request of the state prosecutor, and that a special law will lay down further procedures and detailed conditions to include a person in a protection programme and to conclude the protection programme; the competent bodies deciding on protection and its provision; potential protective measures, records and data protection; funding and supervision of the implementation of protection programmes.

The draft law is being prepared by the working group of the Ministry of Justice, and its drafting is in its final stage; it provides for the establishment of a protection unit at the Ministry of the Interior - Police, and a protection commission, which will operate within the Ministry of Interior and will consist of representatives of the Supreme Court of the Republic of Slovenia, the State Prosecutor General's Office of the Republic of Slovenia, the Ministry of the Interior - Police, and the Ministry of Justice. The draft law also stipulates necessary protective measures[5] and measures within the protection programme[6].

As stated above, article 240a of the Criminal Procedure Act determines the procedure of guaranteeing anonymity associated with hearings before an investigating judge and at the main hearing (i.e. for the purposes of judicial proceedings). The article concerned determines conditions under which the court may order one or more from the five protective measures, which are also determined[7]. Protective measures shall be ordered by the investigating judge, at the written request of the persons concerned. If protective measures are ordered, these data shall be removed from the case records and kept as an official secret. The decision on the use of protective measures may be issued by the investigating judge only after a special hearing has been held, if he believes that appropriate circumstances apply. Article 240a also stipulates that

[5] Counselling of the Unit, technical protection of persons and/or residence, physical protection of persons and/or residence, police measures against potential perpetrators, provisional transfer of persons

[6] transfer of a person, false documents, prohibition of forwarding personal data and control over inquiries into records, covering identity for the purposes of judicial proceedings, change of identity, use of video-conference and telephone conference, international exchange, measures in prison.

[7] deletion of all or certain data from the criminal case records, the marking of the data as an official secret, the assignment of a pseudonym to the witness, and the taking of testimony using technical devices (protective screen, devices for disguising the voice, transmission of sound from separate premises and other similar technical devices)

the above provisions apply mutatis mutandis after the indictment has been submitted to the court and the powers of the investigating judge shall be transferred to the president of the panel.

Effectiveness of border control and controls on preventing access to weapons by terrorists

1.12 The CTC would welcome receiving a progress report in relation to the draft law on amendments to the Law on Foreigners with a view to put in place a more efficient implementation of measures related to the denial of approvals for foreigners, whose residence might be related to the execution of terrorist acts, as explained in Slovenia's annex on "Information Exchange on the Code of Conduct on Political-Military Security Aspects," referred to at page 11 of the first report.

Aliens Act was amended by the Act Amending Aliens Act (Ur. l. RS, No. 87/02 of 17 October 2002) and the Corrigendum to the Act Amending Aliens Act (Ur. l. RS, No. 96/02 of 14 November 2002).

The amendments to the Aliens Act stipulate that an alien who is in possession of a valid travel document and/or a visa, if required, can be refused entry into the country if there are reasonable grounds to suspect that he/she may pose a threat to public order and security or international relations of the Republic of Slovenia, or if there is a suspicion that his/her presence in the country is associated with the carrying-out of terrorist or other violent activities, illegal intelligence activities, drug possession and trafficking, or the carrying-out of other criminal activities.

The suspicion that an alien's presence in the country will be associated with the carrying-out of terrorist or other violent activities, illegal intelligence activities, drug possession and trafficking is defined in detail in the *Instructions on refusal of entry to an alien, conditions for issuing visas at the border, conditions for issuing visas for humanitarian reasons, and regarding the procedure of repealing a visa* (Ur. l. RS, No. 2/01 of 12 January 2001).

Such suspicion is particularly reasonable:

- if he/she is a national of a country where terrorist acts are frequent and if his/her arrival into the country has not been substantiated;
- if there are data which imply the possibility that such an alien is a member of a terrorist organisation;
- if the psycho-physical condition of such an alien indicates that he/she is taking drugs, if he/she is in possession of drugs or equipment used for taking drugs, or
- if it is established that he/she was tried in the Republic of Slovenia or in another country in the period of the preceding two years for a violation or a criminal offence connected with drugs;
- if such an alien is in possession of objects and substances that are used in carrying-out criminal acts.

1.13 In relation to article 79 of the Aliens Act, concerning the conditions for refusal to issue travel documents to aliens, as well as the seizure of aliens, referred to at page 7 of the third report, please outline the conditions, as well as the mechanisms employed in this regard.

Article 79 of the Aliens Act refers to the conditions for refusal to issue passports to aliens and for the seizure of their passports; it does not, however, refer to the arrest of aliens.

According to the applicable Slovenian legislation aliens may be issued with a passport under certain conditions. According to Article 76, par. 1 of the Aliens Act (Ur. l. RS, No. 108/02 –

official consolidated text) a passport for aliens may be issued to an alien who is in possession of a temporary or permanent permit for residence in the Republic of Slovenia, and under the condition that the person concerned is stateless or does not have and cannot acquire a valid travel document from his/her country of origin. A sticker in the passport for aliens marks the previously issued permit for residence that enables an alien not only to reside in the Republic of Slovenia but also to cross the border an unlimited number of times. A passport for aliens may be issued for the time of residence permit validity, but for not more than two years, unless the alien applies for a travel document with a shorter period of validity or a shorter period of validity is sufficient for achieving the purpose for which the travel document is being issued.

Pursuant to Article 76, par. 2 of the Aliens Act a passport for aliens may also be issued to an alien who does not have a valid travel document, if well-founded reasons exist for this. According to the said provision a passport for aliens may be issued to an alien who is leaving the Republic of Slovenia and is not in possession of a travel document of his/her country of origin whereas that country does not have a diplomatic or consular representation in the Republic of Slovenia, and to an alien who has been released from the citizenship of the Republic of Slovenia to leave the country. In such cases a passport for aliens with shorter validity is issued, namely for the time that is necessary for the alien to leave the Republic of Slovenia or to move into another country.

During the administrative procedure for the issuing of a passport for aliens the competent authority verifies if the stipulated conditions for the issuing of a passport for aliens are met and also if there are any reasons for a refusal to issue, referred to in Article 79, par. 1 of the Aliens Act. The competent authority will not issue a passport for aliens:

- to an alien against whom criminal proceedings are in progress, if so requested by the competent court;
- to an alien who has been given an unconditional prison sentence and has not yet served the sentence;
- to an alien who has not settled his/her maintenance liabilities arising from marriage or from relations between parents and children to entitled persons who have permanent residence in the Republic of Slovenia, if so requested by the competent authority; and
- to an alien who has not settled his/her tax liabilities, if so requested by the competent authority.

By refusing the issuing of a passport for aliens for the above reasons, such an alien is prevented to leave the Republic of Slovenia, since his/her presence in the country is required.

Pursuant to Article 79, par. 2 of the Aliens Act a passport for aliens may be seized:

- if subsequent to the issuing of a passport for aliens reasons (specified in Article 79, par. 1 of the Aliens Act) are determined or emerge due to which a passport would not be issued to an alien;
- if the passport does not contain a photograph or if it is no longer possible to determine the identity of the alien; and
- if the passport is forged, incomplete or damaged in some other way.

*1.14 **The effective implementation of subparagraph 2 (a) of the Resolution requires each Member State, inter alia, to have in place an appropriate mechanism to deny terrorists access to weapons. With regard to this requirement of the Resolution, as well as to the provisions of the Convention on the Marking of Plastic Explosives for the purposes of Detection, and International Convention for the Suppression of Terrorist Bombings, please provide the CTC with information relevant to the following questions:***

A) Legislation, regulations, administrative procedures:

- ***What national measures exist to prevent the manufacture, stockpiling, transfer and possession of unmarked or inadequately marked:***
    - ***Plastic explosives;***
    - ***Other explosives and their precursors.***

Pursuant to Article 3 of the Explosive Substances Act (Ur. l. RS, No. 96/02) the following are considered as explosives:

- blasting explosives
- black powder
- explosive preparations
- initiation and ignition devices
- products filled with explosives
- pyrotechnical compounds
- pyrotechnical articles.

The Explosive Substances Act stipulates that only those explosives which are in accordance with the technical requirements and bear adequate markings, and of which conformity has been established following the prescribed procedure, can be placed on the market and can enter into service.

Only legal persons that have acquired special authorisation of the Ministry of the Interior can engage in trading and manufacture of explosives. Furthermore, any purchase of explosives requires a special authorisation by the competent administration unit. Purchase authorisation can only be acquired by a legal person holding marketing authorisation for explosives.

The supervision over the manufacture, storage, transfer and use of explosives is performed by the Police and the Internal Affairs Inspectorate of the Republic of Slovenia. Any explosive that is not in accordance with the technical requirements or is not adequately marked is seized. The possession of such explosive by a person holding a marketing authorisation for explosives is nevertheless considered to be a violation. If, however, such explosive is found in the possession of a person who does not hold a marketing authorisation for explosives, this is considered to be a criminal offence pursuant to Article 310 of the Penal Code of the Republic of Slovenia.

As far as control is concerned both the Police and the Inspectorate have broad powers and can, within their authority, inspect all documentation relating to storage or manufacture of explosives without any prior orders of the court or the court for violations. They may enter on the premises in which explosives are stored and inspect the buildings in which they are manufactured as well as the sites where they are used (Articles 45, 46, 47, 48 and 49 of the Explosive Substances Act).

In the Republic of Slovenia there is no manufacturer of any kind of military explosives, neither plastic nor other types of military explosives. Slovenia has neither an appropriate technology, nor manufacturing bases or capacities. There is also no intention in Slovenia to begin with explosives manufacturing. As a consequence, Slovenia does not take any measures aimed at preventing the manufacture of non-marked plastic or other military explosives or their components. Slovenia does, however, carry out measures to prevent the possession of inadequately marked plastic explosives and precursors; for this purpose it only allows the import/export of properly marked plastic explosives and precursors.

Military explosives are in the exclusive possession of Slovenian Armed Forces, the latter taking all appropriate measures to prevent the transfer and/or possession of inadequately marked plastic explosives. Inadequately marked plastic explosives are destroyed.

B) Export control:

- ***Please specify what export control procedures are used in Slovenia, as well as what mechanism exist for the exchange of information regarding the sources, routs and methods that may be used by arms-traders?***

Trading in military weapons and equipment is regulated by the Defence Act (Ur. l. RS, No. 103/04 – official consolidated text), stipulating that only a company, institution or other organisation that has been granted a licence by the Ministry of Defence may trade in, export or import military weapons and equipment or engage in brokering such goods. Each export, import or transit of military weapons and equipment on the state territory requires a prior authorisation of the Ministry of Defence.

On the basis of the said Act the Government of the Republic of Slovenia issued the Decree on licences and authorisations for traffic and manufacture of military weapons and equipment (Ur. l. RS, No. 18/03 and 31/05). Weapons and equipment are defined in the Decree on armament, military equipment, special operational technique and orders of confidential nature (Ur. l. RS, No. 76/01, 19/05 and 24/05). Trading authorisations are issued by the Ministry of Defence; a specific authorisation by the Ministry of Defence is required for every export, import and transit across the state territory. Such authorisation is issued on the basis of a prior opinion of an expert commission, which is appointed by the Government of the Republic of Slovenia and has to issue its opinion within 30 days from the date of application for the issuing of authorisation. The Ministry may also request a prior opinion from the commission for a single transit. The expert commission includes a representative from the Customs Administration of the Republic of Slovenia. The Ministry issues a final decision on the authorisation for a specific transaction. As a rule, the authorisation for a transaction must be issued at least 3 days prior to the actual transaction. The Ministry also sends the authorisation for a specific transaction to the General Customs Administration. At least 3 days prior to the arrival of goods at the border crossing point, a company, institution or other organisation as well as a sole trader, who has acquired the authorisation for a specific transaction, must forward to the Ministry, the General Police Directorate and the General Customs Administration a written notice stating the date and border crossing point, the number and date of the issued authorisation, the shipping route and the content of shipment.

The so-called "weapons for civilian use" are defined in the Weapons Act (Ur. l. RS, No. 23/05 – official consolidated text), which differentiates between weapons for security, hunting and sports purposes. The Weapons Act makes a conceptual distinction between prohibited and permitted weapons. The Act also stipulates the conditions for the transfer of weapons across the state border that apply to state authorities, companies and other organisations as well as foreign carriers, who may import, export and transfer weapons only with an authorisation from the Ministry of the Interior and with a prior approval of the ministry responsible for defence. The Act further stipulates the conditions for the transfer of weapons across the state border by individuals - natural persons. Registering weapons with border control authorities (Police) does not exclude either the declaration of the weapons to customs authorities or the application of customs regulations.

The import, export and transit of ammunition are subject to the provisions of the Explosive Substances Act. In accordance with the Explosive Substances Act for the import, export and transit of explosives an authorisation is required from the Ministry of the Interior, issued to legal persons or entrepreneurs holding marketing authorisations. Any transit is carried out under customs supervision. The supervision over the application of the Explosive Substances Act is also assured by the Customs service.

On the one hand, the exchange of information on weapons is going on between the responsible authorities in the Republic of Slovenia within the framework of statutory provisions. On the other hand, the Customs service obtains ample information through international institutions

such as Interpol, Europol, the Regional Intelligence Liaison Office (RILO), the Southeast European Cooperative Initiative (SECI) and others, as well as through direct cooperation with customs authorities of other countries.

The Customs service has a proper intranet information system, into which warnings and remarks for diverse sensitive and important areas are entered, including restrictive measures concerning weapons-related pieces of information (violations, irregularities, seizures, observations etc.). Access to this information via the web requires authorisation for all authorised officers of the Customs service. The acquired data and information are entered into the system on a daily basis in the General Customs Administration. The system also enables the entry of urgent and significant information – warnings from the authorised officers of the Customs service that are situated in different locations.

For any export and also import of weapons in the Republic of Slovenia an authorisation is required. The authorisation comprises an annex on which the authority that carries out border control confirms the exit or entry of weapons with a stamp and notifies the competent body that issued the authorisation thereof (Article 71 (d) of the Weapons Act).

Weapons export control is divided into two stages: first there is the administrative procedure, carried out by the Directorate for internal administrative affairs at the Ministry of the Interior (DUNZ), during which the authenticity of statements in the applications is verified. On the basis of return documentation, received from the border police or the holder of the authorisation, the DUNZ may thus subsequently check if a transaction has been really carried out; the Directorate can also request from the country of destination, which has signed the Protocol, to verify if the shipment has actually reached the consignee. The second stage of weapons export control is the administrative control that is carried out by the Police at the moment of declaration of transfer across the state border; essentially, it comprises the comparison of data in the authorisation document with the actual situation at the moment of border crossing. In case of suspicious circumstances, from which the Police could infer that a shipment of weapons may be redirected before reaching the declared consignee or that a shipment actually contains non-declared goods, the Police will thoroughly inspect the shipment at the border crossing point and establish communication with security authorities of the countries through which such shipment would transit or to which it would be exported. Through joint collaboration the police then try to determine the actual circumstances regarding the shipment and/or establish whether the suspicion of illegal activity does or does not have grounds. The information between security authorities in this domain is exchanged through the police cooperation system linking Interpol, Europol, SECI and the Stability Pact for South Eastern Europe. All communications are encrypted. The exchange of data and the verification of suspicious circumstances related to weapon shipments is based on the following ratified international legal instruments:

- European Convention on the Control of Acquisition and Possession of Firearms by Individuals (Ur. l. RS – MP, No. 10/2000 of 21 April 2000),
- Act ratifying the UN Convention against Transnational Organized Crime (Ur. l. RS, No. 41/2004 of 22 April 2004),
- Act ratifying the UN Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, which complements the UN Convention against Transnational Organized Crime (Ur. l. RS – MP, No. 15/04),

and the signed or politically-binding documents:

- OSCE Document on Small Arms and Light Weapons, adopted at the 308th meeting of the OSCE participating states, 24 November 2000,
- Joint Declaration on Responsible Arms Transfers and the Statement on Harmonization of End-Use/End-User Certificates, Stability Pact for South Eastern Europe, Sofia, 15

December 1999, and

- the UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in all its Aspects, adopted at the UN conference in New York, July 2001.

In the Republic of Slovenia the export control of military weapons and equipment is carried out in a coordinated way by the authorities issuing export authorisations, supervisory authorities and intelligence services. This regime has been enabled by the establishment of the Expert commission for the export control of military weapons and equipment, composed of the representatives of the authorities issuing export authorisations, supervisory authorities (Police and Customs service) and intelligence services (Slovenian Intelligence and Security Agency and Intelligence Security Service). The expert commission issues a prior opinion before any issuing of export authorisation for military weapons and equipment. The expert commission also ensures the coordination of activities and exchange of information between the authorities issuing export authorisations, intelligence services and supervisory authorities as regards the sources, routes and methods that may be used by arms-traders.

- ***Is it necessary to lodge, register, or check the Goods Declaration and supporting documents relating to firearms prior to the import, export or transit movement of the goods, as well as encourage importers, exporters or third parties to provide information to Customs prior to their shipment? Please outline also any appropriate mechanism used to verify the authenticity of licensing, or the authorisation of documents for the import, export or transit of firearms?***

The role of the Customs service in the import, export and transit procedures involving military weapons and equipment, weapons for civilian use and explosives is quite clearly defined and significant. Following the acceptance of a customs declaration, which has to be lodged in order to carry out one of the procedures (import, export, transit) for the goods in question, the competent customs authority determines all the requirements provided for acceptance, in compliance with customs laws. It is important that the declaration be lodged by the beneficiary in due form and duly filled in, that any documents required for the approval of the requested procedure be enclosed, and that these documents be issued by competent authorities, be authentic and contain all the data relevant for the procedure requested.

Where required by customs supervision measures the identity of goods is verified, applying measures to ensure the identity of goods. In compliance with customs regulations, samples of goods may be taken to carry out a detailed examination of goods in the General Customs Directorate. The above procedures are carried out in the regular procedure of goods traffic at border crossings and in internal organisational units. The procedures involving passengers who carry over border crossings weapons for their personal use, in particular hunting and sports weapons, also belong to this category.

In effecting control, customs authorities detect, in cooperation with the competent authorities (the Police), irregularities and violations considered either as minor offences or as criminal offences, depending on the actual state of the case in question. The seizure of goods and/or means of transport or delivery is not excluded.

- In addition to the above, the Customs Service also performs, on a regular basis and in compliance with the Customs Service Act (Ur. l. RS, No. 103/04 - official consolidated text) subsequent control and inspection in companies, organisations and sole proprietors possessing permits for the production and traffic of weapons and equipment.

In 2004 the Act Amending the Weapons Act was adopted (Ur. l. RS, No. 73/04), regulating the traffic of weapons across the state border in a uniform manner.

Thereby the provisions of Articles 34 to 42, 44 to 46, Article 58, paragraph 1, items 6 and 7, paragraphs 2 and 3, Article 59, paragraph 1, items 13 and 14 and Article 59, paragraph 2 of the Law on State Border Control (Ur. l. RS, No. 1/91) ceased to apply.

In compliance with applicable legislation, the Police require that the carriers engaged in the transfer of weapons, parts of weapons and ammunition across the state border produce original permits for the import, export or transit of weapons. No traffic of weapons, parts thereof or ammunition is allowed on the basis of copies of such permits.

The Ministry of the Interior issues the permit for the import, export or transit of weapons based on the opinion of the ministry responsible for foreign affairs and the ministry responsible for defence (Article 71 e of the Weapons Act).

The content of the application for issuing an import, export or transit permit is laid down and shall contain:

- name and headquarters of the legal person or sole proprietor,
- identification number of the legal person or sole proprietor,
- quantity of weapons,
- type, brand, marking and calibre of weapons,
- name of weapons manufacturer,
- categorisation of weapons pursuant to Article 3 of the Weapons Act,
- name and address of seller or consignor of weapons and name and address of purchaser or
- consignee,
- purpose of import or export,
- means of transport,
- name and family name of the driver and make and registration number of the vehicle,
- time of import, export or transit,
- border crossing entry or exit point and route,
- import or transit permit of the country into which the weapons are being exported and through which they are transiting.

Individuals are required to bring in or take out weapons at a border crossing stated in the permit; when crossing the border, they are obliged to declare weapons forthwith to the border control authority and submit the specification allowing for the identification of weapons.

In compliance with regulations applicable in the Republic of Slovenia, manufacturers or traders or carriers must, no later than 3 days prior to the import, export or transit of goods, report the transaction to the authority, which issued the permit, the police and customs. On effecting import, export or transit control, the trader or manufacturer or carrier must produce an appropriate permit and declaration of goods as well as documentation relating to the goods. The authority effecting control may check the identity of goods specified in the permit against the goods that are the object of transaction. Following the effected import, export or transit, manufacturers or traders or carriers are bound to report, within 8 days, the transaction to the authority that issued the permit. The latter then controls and registers shipments, deliveries in compliance with indications contained in the permit and informs thereof the authorities effecting control.

- ***Has Slovenia implemented, using risk assessment principle, any special security measures on the import, export and transit of firearms, such as conducting security checks on the temporary storage, warehousing and means of transport of firearms? Are persons involved in these operations required to undergo security vetting? If yes, please give details.***

In Slovenia, control over import, export and transit of weapons is carried out by the Internal Affairs Inspectorate staff members with special powers - weapons inspectors (hereinafter referred to as "the inspector").

The inspector is independent in carrying out inspection supervision, issuing decisions and administrative decisions and order other measures within his/her powers. In order to carry out his/her tasks, the inspector may request the assistance of the Police, Customs and other inspection authorities.

The inspector supervises the implementation of provisions of the Weapons Act with legal persons and sole proprietors who possess weapons, are engaged in weapons traffic or shooting range activity:

- checks matters relating to status;
- checks if general conditions required for weapons possession or traffic or the shooting range activity under this Act have been fulfilled;
- check the suitability of business premises intended for weapons traffic;
- inspects the suitability of warehouses of weapons and ammunition and other places where weapons and ammunition are stored;
- checks the identity of authorised persons and persons working directly with weapons and verifies whether these persons fulfil the conditions for carrying out the work provided for in the Act;
- performs an inspection of prescribed records and other documentation on weapons and ammunition, to buyers of weapons and ammunition and to other persons entrusted with weapons;
- in performing inspection supervision, he/she cooperates with state authorities and organisations as well as with organisations holders of public authority.

Legal persons and sole proprietors who possess weapons, are engaged in weapons traffic or shooting range activity, their responsible persons or persons who were entrusted with weapons or persons directly engaged in work with weapons must allow the inspector unimpeded access to carry out the inspection.

The minister responsible for internal affairs shall issue regulations on carrying out inspection relating to weapons. The provisions of the act regulating inspection supervision and the act regulating the general administrative procedure shall apply to inspectors and to the carrying out of inspection supervision unless otherwise determined by the Act (Article 80 of the Weapons Act).

No security vetting is required for weapons inspectors; they must however pass special examinations relating to their powers, administrative procedure, etc.

In compliance with risk assessment principles, Slovenia is carrying out security measures on the import, export and transit of weapons by monitoring shipments, performing security checks of shipments, etc.

On import, export or transit of weapons across the territory of the Republic of Slovenia and in case of confidential transactions, all persons and companies must undergo appropriate security vetting in compliance with Classified Information Act (Ur. l. RS, No. 135/03 - official consolidated text). A detailed procedure for the security vetting of persons is defined in Articles 22 - 25; the conditions to be fulfilled by a company to receive a security vetting certificate are set out in Article 35 of the Classified Information Act.

Within the systemic use of risk assessment performed by the General Customs Directorate, risk profiles are developed on the basis of collected information, which are then entered in the

Customs Information System (CIS) in the form of instructions directing the customs officer to make further checks of documents and goods when carrying out a specific procedure.

C) Brokering:

- ***Do existing laws require the disclosure of the names and locations of brokers involved in an arms transaction, on either the import and export licenses or authorization, or on any accomplishing documents?***

All entities in the Republic of Slovenia involved in trade in arms are under an obligation to acquire a trade permit. Trade in arms shall mean the purchase of weapons, ammunition and parts of weapons, and their further wholesale and retail sale, brokering the purchase and sale of weapons, their storage and maintenance. The same conditions apply to brokering as in the case of an application for import, export or transit.

If there are grounds for suspicion that illegal activity is involved, the police may acquire data on an individual permit issued; the police shall protect such information in compliance with the Personal Data Protection Act and the Police Act (Ur. l. RS, No. 102/04 - official consolidated text and No. 14/05 - amendment to the official consolidated text).

In compliance with regulations applicable in the Republic of Slovenia, Slovenian companies engaged in brokering must posses the appropriate permit. In acquiring a brokering permit, the names and locations of brokers must be disclosed. When issuing import and export permits the disclosure of the names and locations of brokers is required as well as an appropriate registration of brokers by states in which they carry out business activities or in which they are registered.

- ***Are there legal provisions in place to allow for the sharing of relevant information with foreign counterparts to enable cooperation in preventing illegal shipment of firearms, their parts and components and ammunition, as well as explosives and their precursors?***

If there are grounds for suspicion that illegal activities are involved, the Slovenian Police verifies circumstances through Interpol and Europol. There are no limitations to international police cooperation; any transfer of personal data outside the country must be duly recorded and legally justified.

The exchange of information between security and intelligence agencies regarding the shipments of weapons, weapons of mass destruction and similar is almost always defined in security agreements signed by states at the bilateral basis. This ensures that important data will not be disclosed to a third party. Slovenia exchanges such data with NATO and the European Union on the basis of the signed and ratified security agreements. Slovenia also concluded such an agreement with the US. It was signed in 1996 and applies since 1997.

D) Law enforcement / illegal trafficking:

- ***The CTC notes Article 9 of the Aliens Act, referred to at page 10 of the first report, includes the refusal of the entry of aliens if there is suspicion that their presence may be associated with illegal trafficking. The CTC, however, would appreciate learning what other specific measures are used by Slovenia to prevent and suppress illegal trafficking in firearms, ammunition, and explosives, which can be utilized by terrorists?***

When investigating criminal offences and collecting evidence, the Police may use secret surveillance measures (see answer 10.1). When investigating criminal offences the Police also

use other, classical methods of policing, such as international police cooperation, control of vehicles, baggage and persons at state border, control of passengers and baggage in the country if grounds exist to suspect that a criminal offence was committed, as well as other police measures. In police procedures and legal proceedings, Slovenian legislation does not draw a distinction between "classical" and "terrorist" criminal offences; in dealing with and investigating criminal offences, the court and police procedures are the same regardless of the type of criminal offence.

- ***The CTC would welcome receiving a progress report regarding the amendments to the Slovenia Arms Act to be in compliance with the UN Convention against Transnational Organised Crime and the protocol on the Prevention of Illegal Arms Trade, as indicated at page 7 of Slovenia's report, submitted pursuant to Resolution 1455 (2003), to which a reference is made at page 9 of the third report to the CTC.***

The Weapons Act was completely harmonised with the above-mentioned international legal instruments in 2001.

On the basis of international sources, Article 310 of the Criminal Code of the Republic of Slovenia, dealing with unlawful production and sale of weapons or explosives was also amended in 2004. The notion of "brokering" in weapons transactions is also stated under this criminal offence. International legal instruments ratified in the Republic of Slovenia (Protocol to the UN Convention against the International Organised Crime and the European Convention on the control of the acquisition and possession of firearms by individuals) are part of the Slovenian legal order and therefore, their provisions have not been included in the Weapons Act.

1.15 ***The effective implementation of subparagraph 2 (e) of the Resolution requires each Member State, inter alia, to have in place national provisions to enable it to stand ready to cooperate with other States as well as to examine foreign requests for cooperation promptly. In this regard, the CTC notes that the Code of Criminal procedure in Slovenia devotes a special chapter to extradition (Article 521 - 536) with a view to foreseeing solution regarding both the conditions for extradition, as well as the individual proceedings, as explained throughout pages 9 and 10 of the first report. The CTC has also taken note of Slovenia's domestic provisions regulating international legal assistance as outlined throughout pages 8 and 9 of the first report. In this regard, the CTC is also interested in being provided with similar outline and explanation of provisions that govern the freezing of funds of illicit origin and/or of legal origin suspected to be used for the commission of terrorist acts, pursuant to a request submitted by foreign State. In addition, please explain to the CTC if there are any situations in which the Office for Money Laundering Prevention in Slovenia may play a role in this regard.***

Article 515, paragraph 1 of the Criminal Procedure Act stipulates that foreign requests for legal assistance shall be transmitted through diplomatic channels. Paragraph 2 of the same Article stipulates, in relation to the Office for the Prevention of Money Laundering, to which the request for additional information refers, that in emergency cases and on condition of reciprocity, requests for legal assistance in instances of criminal offences of money laundering or criminal offences connected to the criminal offence of money laundering (e.g. predicate criminal offences), may also be sent to the body responsible for the prevention of money laundering.

The Office of the Republic of Slovenia for the Prevention of Money Laundering is authorised to issue, on the basis of Article 16 of the Prevention of Money Laundering Act a written order temporarily postponing a transaction for no longer than 72 hours if it believes that there exist well-founded reasons to suspect money laundering and inform the competent bodies thereof

(Police, State Prosecutor's Office). The Office may make use of authority to temporarily postpone a transaction only in cases where there exist well-founded reasons to suspect money laundering, which means that the Police and the State Prosecutor's Office will probably initiate a preliminary procedure (police procedure, investigation, investigating acts, etc.). The Office could also make use of authorisation to temporarily postpone a transaction in cases involving money laundering deriving from the financing of terrorism or other terrorist acts. Upon the amendment to the Prevention of Money Laundering Act, the Office will also obtain the power to block (for 72 hours) the transactions relating solely to the financing of terrorism or terrorist organisations.

With reference to the seizure of money and property, the Office is designated, on the basis of the Act ratifying the Council of Europe Convention No. 141 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Ur. l. RS-MP, No. 11/97 and 8/98), as the central authority through which international requests are transmitted.

1.16 ***The CTC would like to emphasize that it appreciate receiving copies of any reports or questionnaires submitted to other organizations involved in monitoring international standard as part of Slovenia's response to the points in the preceding paragraphs, as well as details of any efforts to implement international best practices, codes and standards which are relevant to the implementation of the Resolution.***

The Republic of Slovenia has recently submitted replies to the questionnaires of the European Union, the Council of Europe and other international organisations. All reports have been marked as classified by the relevant organisations, therefore, Slovenia cannot submit them without prior consent of these organisations.